FMV IŞIK ÜNİVERSİTESİ

GÜVENLİK DUVARI YENİLEME VE AĞ OTOMASYON YAZILIMI ALIM İHALESİ

TEKNİK ŞARTNAMESİ

Genel Kapsam

- Bu ihale kapsamında kısmı teklif verilemez, firmalar bütün ürün ve kapsam için teklif verecektir.
- Bu ihale kapsamında konsorsiyum yapı kabul edilmeyecektir.
- Teklif edilecek Firewall Cihazı, Network Otomasyon yazılımı ile uyumlu olacaktır.
- Teklif edilen ürünlerin (donanım+yazılım) kurulumları, konfigürasyonları ve mevcut sistemden aktarım gerekirse bu işlemleri teklif dahilindedir. Mevcut altyapıdaki donanım ve yazılım eksikleri yüklenici sorumluluğunda olacaktır ve ekstra bir ücret talep edilmeden kurumun ihtiyacı giderilecektir.

1. Şile Kampüs Firewall Teknik Özellikleri (2 Adet)

Ağ Güvenlik Duvarı aşağıda belirtilen güvenlik fonksiyonlarını ve teknolojilerini sağlamalıdır.

1.1. Teklif edilen sistem, yeni nesil güvenlik duvarı özellikleri olarak asgari;

1.1.1. Güvenlik Duvarı (Firewall)
1.1.2. IPSec VPN Sonlandırma Sistemi
1.1.3. SSL VPN Sonlandırma Sistemi
1.1.4. Saldırı Tespit ve Engelleme Sistemi (IPS)
1.1.5. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
1.1.6. Virüs/Zararlı İçerik Kontrolü
1.1.7. URL Kategori Filtreleme
1.1.8. Bant genişliği yönetimi

Özelliklerine sahip olmalıdır.

1.2. Bu özellikleri üreticiye ait donanımsal çözüm olarak tek bir cihaz ile sağlamalıdır. Fakat IPSec VPN ve SSL VPN özelliklerinin Transparan konumlandırıldığında desteklenememesi durumda; aynı sistem üzerinde sanal güvenlik duvarı özelliği ile veya aynı üreticiye ait ayrı bir donanımsal ürün ile sağlanabilir.

1.3. Cihaz tek bir fiziksel güvenlik duvarı olarak çalışabileceği gibi, herhalukarda kurumun ihtiyaç duyması durumunda en az 10 adet sanal güvenlik duvarı çalıştıracak şekilde konfigüre edilebilmelidir.

1.4. Teklif edilen Ağ Güvenlik Duvarı High-Availability için Aktif-Aktif ve Aktif-Pasif olarak çalışmayı desteklemelidir. Aktif-Aktif çalışırken yük paylaşımı yapabilmelidir. Cihazlardan birinin arızalanması durumunda, diğer cihaz tüm fonksiyonları üstlenerek çalışmaya devam edebilmelidir.

1.5. Yedeklilik konfügrasyonunda her segment için güvenlik duvarı üzerinde set edilecek Ip sayısı 1 (bir) adet olmalıdır. Bu sayede modüller için ayrı, cluster IP si için ayrı IP adreslerinin kullanımına gerek kalmamalıdır.

1.6. Sistemin SPI (Stateful Packet Inspection) Firewall özelliği olmalıdır.

1.7. Sistem, spoof edilmiş paketleri tespit edip bloklayacaktır

1.8. Sistemde bulunan ağ arayüzlerinin her biri; LAN, WAN, DMZ, veya kullanıcı tarafından isimlendirilebilen segmentler olarak tanımlanabilmelidir. Sistem IEEE 802.1Q VLAN desteklemeli ve tanımlanan VLAN'lar arayüz (interface) olarak kullanılabilmelidir.

1.9. Sistem Sanal Güvenlik Duvarı özelliği ile kullanıldığı durumda; sistem üzerindeki fiziksel ve sanal ara yüzler Sanal Güvenlik Duvarları arasında paylaştırılabilmelidir. Sanal Güvenlik Duvarları kural ve yönlendirme açısından birbirinden bağımsız olarak yönetilebilmelidir.

1.10. Sistem; Layer3 (routing mod) ve Layer2 (saydam mod) katmanlarında çalışabilmelidir. Sistem üzerinde sanal güvenlik duvarı sistemlerinden istenilenler Layer3 te çalışabilirken aynı anda istenilen sanal güvenlik duvarları Layer2 de transparant olarak çalışabilmelidir.

1.11. Saydam (Transparent) modda aşağıdaki özellikleri sağlamalıdır;
- 1.11.1. SPI (stateful packet inspection),
- 1.11.2. Saldırı Tespit ve Engelleme Sistemi (IPS)
- 1.11.3. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
- 1.11.4. Ağ Geçidinde Virüs/Zararlı İçerik Kontrolü
- 1.11.5. URL Kategori Filtreleme

1.12. Routing modda aşağıdaki özellikleri sağlamalıdır;
- 1.12.1. SPI (stateful packet inspection),
- 1.12.2. IPSec VPN Sonlandırma,
- 1.12.3. SSL VPN Sonlandırma,
- 1.12.4. Saldırı Tespit ve Engelleme Sistemi (IPS)
- 1.12.5. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
- 1.12.6. Virüs/Zararlı İçerik Kontrolü
- 1.12.7. URL Kategori Filtreleme
- 1.12.8. Bant genişliği kontrolü
- 1.12.9. Statik yönlendirme (static routing),
- 1.12.10. RIP, OSPF ve BGP yönlendirme protokollerini desteklemelidir. Bu yönlendirme protokollerini sağlamak için lisans veya fazladan yazılım gerekiyorsa sağlanmış olmalıdır.
- 1.12.11. Sunucu yük dengeleme
- 1.12.12. WIFI Access Point kontrolcüsü
- 1.12.13. WAN optimizasyon
- 1.12.14. Web Cache

1.13. Ağ Güvenlik Sisteminin, Birden fazla Geniş Alan Ağı (WAN) bağlantısını desteklemeli, birden fazla Internet bağlantısını yedekli ve/veya aynı anda kullanabilmelidir.

1.14. Ağ Güvenlik Sistemi, Kural Tabanlı Yönlendirmeyi (Policy Based Routing) desteklemelidir.

1.15. Sistemin DHCP Server ve DHCP Relay özelliği bulunmalıdır.

1.16. Güvenlik duvarı politikaları sistem üzerindeki ağ arayüzü ve/veya zone bazlı yazılabilmelidir.

1.17. Güvenlik duvarı politikaları, kullanıcı grupları bazında yazılabilmeldir. Kullanıcı bilgisi için AD entegrasyonu olmalıdır.

1.18. Kullanıcı bazında NAT kuralı yazılabilmelidir.

1.19. Sistem Bant Genişliği Kontrolü amacıyla kural tabanlı trafik biçimlendirme ve trafik önceliklendirme yapabilmelidir. Sistem QoS ve Differentiated Services desteklemelidir.

1.19.1. Kaynak, hedef ve protokol (SMTP, FTP, DNS, H323 gibi) bazında yazılan kurallarda trafik biçimlendirme tanımı da yapılabilmelidir.
1.19.2. Maksimum ve/veya garanti edilecek bant genişliği değeri öncelik değeri (düşük, orta, yüksek gibi) ile tanımlanabilmelidir.
1.19.3. İstenildiğinde tek IP bazında bant genişliği kontrolü yapılabilmelidir. Bu sayede aynı kural dahilinde izin verilmiş olan tüm kaynak IP lerin herbiri için, tanımlanan bant genişliğinin ve/veya max eşzamanlı oturum sayısının garanti edilmesi sağlanmalıdır.
1.19.4. Aynı kural dahilinde izin verilen her kaynak için, tanımlanan bant genişliğinin ortak bir şekilde kullanılabilmesi sağlanabilmelidir.
1.19.5. Uygulama bazında bant genişliği kontrolü yapabilmelidir.
1.19.6. Aynı trafik ile ilgili Inbound ve outbound doğrultuda band genişliği kontrolü yapılabilmelidir. Bu sayede izin verilen bir bağlantı için gidiş doğrultusunda bant genişliği belirtilebilirken, bu bağlantıya karşılık gelen trafik için farklı bir bant genişliği uygulanabilmelidir.

1.20. Güvenlik Sistemi; kendi üzerinde tanımlanan kullanıcı veritabanı, RADIUS ve LDAP üzerinden kimlik doğrulama ve yetkilendirme yapabilmelidir.

1.21. Sistemin uygulama kontrol özelliği bulunmalıdır. Sistem; Mesajlaşma (MSN, ICQ, Yahoo, AOL gibi), P2P (Kazaa, Skype, bitTorrent, eDonkey, Gnutella vb) ve Web Uygulamaları gibi tanımlı en az 3.000 (üçbin) adet uygulamaya ait trafiği kullanılan porttan bağımsız olarak tanıyabilmeli, kontrol edebilmeli ve engelleyebilmelidir. Uygulama kontrolü kapsamında tanınan uygulamalar internet üzerinden güncelleme servisi ile güncellenmelidir.

1.22. Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında uygulama kontrol politikası set edilebilmelidir.

1.23. Sistem VPN Gateway olarak IPSec VPN desteklemelidir. DES, 3DES, AES Kriptolama ile MD5 ve SHA-1 desteklemelidir. IKE ve PKI desteği olmalıdır.

1.24. IPS sistemi Trafik ve Protokol anomalilerini tespit edip durdurabildiği gibi, imza tabanlı saldırıları da tanıyıp durdurabilmelidir. IPS imzaları otomatik olarak internet üzerinden güncelleme servisi ile güncellenebilmelidir. Güncelleme işlemi manuel olarak ta yapılabilmelidir.

1.25. Teklif edilen sistem istenilen atak türleri gerçekleştiğinde bu atakları sadece engellemekle kalmayıp, atak kaynağını belli bir süre engelleyebilecek şekilde yapılandırılabilmelidir. Bu sayede atak yapan IP adresinin olası diğer saldırıları başlamadan engellenmiş olmalıdır.

1.26. Sistem yöneticilerinin kuruma/ihtiyaca özel zaafiyet imzaları yaratıp bloklama yapabilmelerine imkân sağlamalıdır.

1.27. Kaynak (IP ve/veya kullanıcı), hedef, servis bazında yazılan her güvenlik duvarı kuralında IPS politikası set edilebilmelidir.

1.28. Teklif edilen Ağ güvenlik sistemi Botnet aktivitesini tespit edip engelleyebilmelidir.

1.29. Ağ Güvenliği Sistemi üzerinde, Mobil Kullanıcıların Kurum kaynaklarına güvenli olarak erişimini sağlayabilmek için, SSL VPN Gateway özelliği bulunmalıdır. SSL VPN istemcisi en az Windows, Mac OS, Linux işletim sistemlerini ve IOS, Android tabanlı mobil cihazları desteklemelidir.

1.30. SSL VPN Gateway içerisinden TCP ve UDP tabanlı trafikler tünellenebilmelidir.

1.31. SSL VPN özelliği en az 500 kullanıcı lisansı ile teklif edilecektir.

1.32. SSL VPN üzerinden erişen kullanıcılar, Sistem üzerinde tanımlı kullanıcı veritabanı, RADIUS, LDAP üzerinden kimlikleri doğrulanabilmeli, yetkilendirilebilmeli ve bu yetkilendirme ile erişilebilecek kurum içi ve dışı kaynaklar tanımlanabilmelidir.

1.33. SSL VPN ile erişim sağlayan kullanıcı veya sistemleri için; SPI (stateful packet inspection), Saldırı Tespit ve Engelleme Sistemi (IPS), Uygulama Tanıma ve Kontrolü (Application Control) Sistemi, Virüs/Zararlı İçerik Kontrolü ve URL Kategori Filtreleme, Bant Genişliği yönetimi (QoS) özellikleri uygulanabilir olmalıdır.

1.34. Ağ Güvenlik Duvarı Sistemi üzerinde zararlı yazılım (Malware) tespit ve engelleme özelliği bulunmalıdır. Sistem; HTTP, SMTP, FTP ve POP3 trafiğini tarayarak zararlı yazılımları engelleyebilmelidir. Sistem, anılan protokoller içinde tarama yaparak; Worm, Trojan, Keylogger, Spy, Dialer türünden tehditleri tanıyıp durdurabilmelidir. Virüs Kontrolü, Ağ Güvenlik Duvarı Sistemi üzerinde bulunan bütün network segment'leri arasında yapılabilmelidir. AntiVirus sistemi Internet üzerinden virüs imzalarını otomatik olarak güncelleyebilmelidir

1.35. Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında AV kontrol politikası set edilebilmelidir.

1.36. Ağ Güvenliği Sistemi üzerinde URL Filtreleme özelliği bulunmalıdır. Bu sayede Kategori bazlı URL Filtreleme yapabilmelidir. Farklı kullanıcı ve kullanıcı gruplarına farklı kategorilerde URL filtreleme uygulanabilmelidir.

1.37. Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında farklı URL filtreleme politikaları set edilebilmelidir.

1.38. Sistem üzerinde en az 60 adet URL kategorisi bulunmalıdır.

1.39. Sistemin URL Filtreleme fonksiyonu için kullanıcı sınırı olmamalı ve sınırsız kullanıcı lisansı ile teklif edilmelidir.

1.40. URL filtreleme kategorileri dışında, wildcard, regex veya tam URL olarak istenilen adreslerin farklı profiller altında tanımları yapılabilmelidir (Örneğin *.gov.tr* gibi). Tanımı yapılan bu adreslere erişim engellenebilmeli veya izin verilebilmelidir.

1.41. İstenildiğinde categorilerden bağımsız olarak, sisteme eklenebilecek tam URL bilgisi (Örneğin: www.abc.com/deneme/sayfa1.php) bazında engelleme yapabilmelidir.

1.42. Https üzerinden erişilmeye çalışılan domain adreslerinin (örneğin www.abc.com) engellemesi sertifika kullanımı olmadan gerçekleştirilebilmelidir.

1.43. SSL trafiğini kendi üzerinde yaratılan bir sertifikayı yada farklı bir CA den alınmış yeterli özelliklere sahip bir sertifika ile inceleyebilmelidir. Bu sayede sadece domain bazında değil, URL bazında (Örneğin: www.abc.com/deneme/test.php) engelleme yapabilmelidir. URL kategorileri bazında SSL incelemeye girmeyecek domainler belirlenebilmelidir.

1.44. URL filtreleme uyarı ekranları özelleştirilebilecektir.

1.45. Teklif edilen tüm sistemlerin IPv6 desteği bulunmalıdır ve IPv4 ile IPv6 protokollerinin aynı anda kullanımına izin veren dual-stack özelliği desteklenmelidir. IPv6 kapsamında en az; IPv6 adresleme, IPv6 statik yönlendirme, IPv6 DNS, IPv6 güvenlik kuralları, IPv6 kayıt ve raporlama ve Ping6 desteklenmelidir.

1.46. Sistem yapılandırması en az aşağıdaki yöntemler ile yapılabilmelidir:
- 1.46.1. Seri bağlantı ile konsol port üzerinden,
- 1.46.2. Http ve Https bağlantı ile web ara yüz üzerinden veya üreticinin kendisine ait Linux veya Windows tabanlı yönetim uygulaması üzerinden
- 1.46.3. SSH bağlantı ile komut satırı (commandline) üzerinden

1.47. Ağ Güvenlik Duvarı Sistemin SNMP desteği olmalı ve SNMPv3 desteklemelidir

1.48. Ağ Güvenlik Duvarı Sistemi işletim sistemi ve yazılım güncellemelerini Web ara yüzü, TFTP veya FTP üzerinden yapılabilmelidir.

1.49. Yedekli olarak çalışan sistemlerin güncellemeleri en az web gui üzerinden yapılabilmelidir. Sistemler otomatik olarak, trafiği kesintiye uğratmayacak şekilde sırayla güncellenebilmelidir.

1.50. Önerilecek güvenlik duvarı sistemi üreticisinin, bir veya birden fazla ürünü, “NSS Labs Network IPS” veya “NSS Labs Next Generation Firewall” testlerine girmiş olması gereklidir.

1.51. Teklif edilen Ağ Güvenlik Duvarı Sistemi üreticisi, güncel “Enterprise Firewall” için “Gartner Magic Quadrant” tablosunda “Leaders” kısmında yer almalıdır.

1.52. Güvenlik Duvarı Sisteminin coğrafi veri tabanı bulunmalıdır. Ülke bazında kural yazılarak belirtilen ülke veya ülkelerden gelen trafiği kesebilmelidir.

1.53. Teklif edilen güvenlik sistemi, aynı zamanda yük dengeliyici özelliklerine sahip olacaktır.

- 1.53.1. Layer 7 için HTTP, HTTPS, SSL, Layer 4 için TCP ve UDP, Layer 3 için IP protokolü bazında tüm oturumlar için yük dengelemesi yapabilmelidir.
- 1.53.2. Yük dengelemesi uygulanan sunucular için IPS, AV politikaları kullanılabilmelidir.
- 1.53.3. HTTP, HTTPS bağlantıları için fiziksel sunuculara kaynak IP adresinin gitmesi sağlanabilmelidir.
- 1.53.4. SSL bağlantıları için SSL Offloading özelliği olmalıdır.
- 1.53.5. Trafik kurum gerçek sunucularına aşağıdaki yöntemlerle dağıtılabilmelidir:
  - 1.53.5.1. Kaynak Ip hash bilgisi

1.53.5.2. Round robin
1.53.5.3. Sunucuların farklı güçlerde olabilme ihtimaline karşı gerçek sunucu tanımlarında ağırlık tanımı yapılarak
1.53.5.4. Aktif durumda olan gerçek sunuculardan ilkine trafiğin gönderilip, devre dışı kalması durumunda sonraki aktif sunucuya yükün gönderimesi
1.53.5.5. Ping paketlerine verilen cevaplar esas alınması
1.53.5.6. Sunucular üzerine yönlendirilen session sayı bilgisine bağlı olarak

1.53.6. Yük paylaşımı sırasında sunucu bulunurluğunu tcp, http (örneğin http://10.31.101.30/test_page.htm adresinin kontrolü ile) ve ping ile kontrol edebilmelidir.

1.54. Belirlenen sistemler üzerinde zaafiyet tarama testi yapabilmelidir.

1.55. Teklif edilen sistem wifi controller olarak çalışabilecek, bu sayede kullanılabilecek kablosuz erişim cihazlarının yönetimi için kullanılabilecektir.

1.56. Wan optimizasyon özelliklerine sahip olacaktır.

1.57. Common Internet File System (CIFS), FTP, HTTP, MAPI ve TCP oturumları için protokol optimizasyonu yapabilmelidir.

1.58. Web cache özelliği olmalıdır.

1.59. Web cache communication Protocol (WCCP) desteği olmalıdır.

a. Güvenlik Duvarı Performans Değerleri

1.1. Teklif edilen güvenlik sistemi, teklif edilen konfigürasyonda, en az 27 Gbps Firewall performansı değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.

1.2. Sistem aynı anda en az 3 milyon oturumu desteklemeli ve saniyede en az 250.000 yeni oturum açabilme performansına sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.

1.3. Her bir Ağ Güvenlik Duvarı ünitesi (cluster içerisindeki herbir cihaz/kart ayrı ayrı olmak üzere) Tehdit Koruma (Firewall + IPS + Uygulama Denetimi + Antimalware) özellikleri aktifken en az **3 Gbps** kapasiteye sahip olmalıdır. Bu kapasite kullanıcı/istemci arasındaki istek-cevap trafiğinin toplamına (**çift yönlü analiz ile**) bu güvenlik özelliklerinin uygulandığı konfigürasyonda belirlenmiş olmalıdır. Belirtilen bu değer ürün kataloglarında yer almalıdır. Ürün kataloglarında Tehdit Koruma için farklı terminoloji kullanılmış ise bu koşulda ürün kataloğunda NGFW (Firewall + IPS + Uygulama Denetimi) kapasitesi gerçek ortam değeri baz alınarak en az **3,5 Gbps** olmalıdır.

1.4. Güvenlik Duvarı Sistemi en az 13 Gbps IPSec VPN throughput değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.

1.5. Güvenlik Duvarı Sistemi en az 2 Gbps SSL VPN throughput değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.

1.6. Sistem Site-to-Site için en az 2.000 adet, Client to site için 5.000 adet IPSec VPN tünel desteklemelidir. Cihaz, anılan VPN protokollerini destekleyen standartlarla uyumlu VPN Gateway cihazları ile uyumlu çalışabilmelidir

1.7. Sistem en az 5 Gbps IPS throughput performans değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.

1.8. Sistem üzerinde;
   1.8.1. En az 4 adet 10 GE SFP+ ara yüz desteği olmalıdır.
   1.8.2. En az 16 adet Gigabit Ethernet RJ45 ara yüz desteği olmalıdır.
   1.8.3. En az 8 adet 1 GE SFP ara yüz desteği olmalıdır.

1.9. Sistem Syslog Sunuculara, Sistem ile birlikte teklif edilecek Kayıt/Raporlama Sistemine kayıt gönderebilmelidir.

1.10. Sistemin; Firewall, VPN, IPS fonksiyonlarının hiç biri için kullanıcı sınırı olmamalıdır ve sınırsız kullanıcı lisansı ile teklif edilmelidir. Ağ Güvenlik Sisteminin 3 yıl süre ile Yazılım/işletim sistemi güncellemelerini ve en az 3 yıl süre için IPS, Uygulama Tanıma ve Kontrolü, AntiVirus, URL Kategori Filtreleme servis ve güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.

2. Maslak Kampüs Firewall Teknik Özellikleri (1 Adet)

2.1. Ağ Güvenlik Duvarı aşağıda belirtilen güvenlik fonksiyonlarını ve teknolojilerini sağlamalıdır.
Teklif edilen sistem, yeni nesil güvenlik duvarı özellikleri olarak asgari;

i. Güvenlik Duvarı (Firewall)
ii. IPSec VPN Sonlandırma Sistemi
iii. SSL VPN Sonlandırma Sistemi
iv. Saldırı Tespit ve Engelleme Sistemi (IPS)
v. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
vi. Virüs/Zararlı İçerik Kontrolü
vii. URL Kategori Filtreleme
viii. Bant genişliği yönetimi

Özelliklerine sahip olmalıdır.

2.2. Bu özellikleri üreticiye ait donanımsal çözüm olarak tek bir cihaz ile sağlamalıdır. Fakat IPSec VPN ve SSL VPN özelliklerinin Transparan konumlandırıldığında desteklenememesi durumda; aynı sistem üzerinde sanal güvenlik duvarı özelliği ile veya aynı üreticiye ait ayrı bir donanımsal ürün ile sağlanabilir.
2.3. Cihaz tek bir fiziksel güvenlik duvarı olarak çalışabileceği gibi, herhalukarda kurumun ihtiyaç duyması durumunda en az 10 adet sanal güvenlik duvarı çalıştıracak şekilde konfigüre edilebilmelidir.
2.4. Yedeklilik konfügrasyonunda her segment için güvenlik duvarı üzerinde set edilecek Ip sayısı 1 (bir) adet olabilmelidir. Bu sayede modüller için ayrı, cluster IP si için ayrı IP adreslerinin kullanımına gerek kalmamalıdır.
2.5. Sistem üzerinde en az 4 adet SFP, 16 Adet RJ45 1Gbit/s interface olmalıdır.
2.6.

2.7. Sistem üzerinde en az 2 adet SFP+ 10Gbit/s interface olmalıdır.
2.8. Sistem üzerinde 2 adet yedekli AC güç kaynağı bulunmalıdır.
2.9. Sistemin SPI (Stateful Packet Inspection) Firewall özelliği olmalıdır.
2.10. Sistem, spoof edilmiş paketleri tespit edip bloklayacaktır, anti-spoof özelliğine sahip olmalıdır.
2.11. Sistemde bulunan ağ arayüzlerinin her biri; LAN, WAN, DMZ, veya kullanıcı tarafından isimlendirilebilen segmentler olarak tanımlanabilmelidir. Sistem IEEE 802.1Q VLAN desteklemeli ve tanımlanan VLAN'lar arayüz (interface) olarak kullanılabilmelidir.
2.12. Sistem Sanal Güvenlik Duvarı özelliği ile kullanıldığı durumda; sistem üzerindeki fiziksel ve sanal ara yüzler Sanal Güvenlik Duvarları arasında paylaştırılabilmelidir. Sanal Güvenlik Duvarları kural ve yönlendirme açısından birbirinden bağımsız olarak yönetilebilmelidir.
2.13. Sistem; Layer3 (routing mod) ve Layer2 (saydam mod) katmanlarında çalışabilmelidir. Sistem üzerinde sanal güvenlik duvarı sistemlerinden istenilenler Layer3 te çalışabilirken aynı anda istenilen sanal güvenlik duvarları Layer2 de transparant olarak çalışabilmelidir.
2.14. Saydam (Transparent) modda aşağıdaki özellikleri sağlamalıdır;

ix. SPI (stateful packet inspection),
x. Saldırı Tespit ve Engelleme Sistemi (IPS)
xi. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
xii. Ağ Geçidinde Virüs/Zararlı İçerik Kontrolü
xiii. URL Kategori Filtreleme

2.15. Routing modda aşağıdaki özellikleri sağlamalıdır;

xiv. SPI (stateful packet inspection),
xv. IPSec VPN Sonlandırma,
xvi. SSL VPN Sonlandırma,
xvii. Saldırı Tespit ve Engelleme Sistemi (IPS)
xviii. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
xix. Virüs/Zararlı İçerik Kontrolü
xx. URL Kategori Filtreleme
xxi. Bant genişliği kontrolü
xxii. Statik yönlendirme (static routing),
xxiii. RIP, OSPF ve BGP yönlendirme protokollerini desteklemelidir. Bu yönlendirme protokollerini sağlamak için lisans veya fazladan yazılım gerekiyorsa sağlanmış olmalıdır.
xxiv. Sunucu yük dengeleme

2.16. Ağ Güvenlik Sisteminin, Birden fazla Geniş Alan Ağı (WAN) bağlantısını desteklemeli, birden fazla Internet bağlantısını yedekli ve/veya aynı anda kullanabilmelidir.
2.17. Ağ Güvenlik Sistemi, Kural Tabanlı Yönlendirmeyi (Policy Based Routing) desteklemelidir.
2.18. Sistemin DHCP Server ve DHCP Relay özelliği bulunmalıdır.
2.19. Güvenlik duvarı politikaları sistem üzerindeki ağ arayüzü (interface) ve/veya zone bazlı yazılabilmelidir.
2.20. Güvenlik duvarı politikaları, kullanıcı grupları bazında yazılabilmeldir. Kullanıcı bilgisi için AD entegrasyonu olmalıdır.
2.21. Kullanıcı bazında NAT kuralı yazılabilmelidir.
2.22. Sistem Bant Genişliği Kontrolü amacıyla kural tabanlı trafik biçimlendirme ve trafik önceliklendirme yapabilmelidir. Sistem QoS ve Differentiated Services desteklemelidir.

xxv. Kaynak, hedef ve protokol (SMTP, FTP, DNS, H323 gibi) bazında yazılan kurallarda trafik biçimlendirme tanımı da yapılabilmelidir.

xxvi. Maksimum ve/veya garanti edilecek bant genişliği değeri öncelik değeri (düşük, orta, yüksek gibi) ile tanımlanabilmelidir.

xxvii. İstenildiğinde tek IP bazında bant genişliği kontrolü yapılabilmelidir. Bu sayede aynı kural dahilinde izin verilmiş olan tüm kaynak IP lerin herbiri için, tanımlanan bant genişliğinin ve/veya max eşzamanlı oturum sayısının garanti edilmesi sağlanmalıdır.

xxviii. Aynı kural dahilinde izin verilen her kaynak için, tanımlanan bant genişliğinin ortak bir şekilde kullanılabilmesi sağlanabilmelidir.

xxix. Uygulama bazında bant genişliği kontrolü yapabilmelidir.

xxx. Aynı trafik ile ilgili Inbound ve outbound doğrultuda band genişliği kontrolü yapılabilmelidir. Bu sayede izin verilen bir bağlantı için gidiş doğrultusunda bant genişliği belirtilebilirken, bu bağlantıya karşılık gelen trafik için farklı bir bant genişliği uygulanabilmelidir.

2.23. Ağ Güvenlik Duvarı Sistemi kendi üzerinde tanımlanan kullanıcı veritabanı, harici RADIUS ve LDAP sunucuları üzerinden kimlik doğrulama ve yetkilendirme yapabilmelidir. SSLVPN, client-site IPSEC VPN, internet erişimi gibi senaryolar için bu özellik kural bazlı devreye alınabilmeli ve kullanıcı takibi (kullanıcı ismi, grubu, yarattığı trafik, kalan süre vb..) gibi detaylar GUI üzerinden gözlemlenebilmelidir.

2.24. Aktif dizin entegrasyonu ağ güvenlik duvarı üzerinden sorgu çekme yöntemiyle veya domain üyesi herhangi bir sunucu üzerine kurulacak ajan yardımıyla gerçekleşebilmelidir. Sistemin temel çalışmasında son kullanıcı makinalarına bir yazılım kurulması ihtiyacı bulunmamalıdır.

2.25. Domain entegrasyonu sonucunda bir nedenden (Windows ortamı vb..) firewall ile senkronize edilememiş kullanıcıların firewall üzerinden geçerken anında tanınabilmesi için NTLMv2 gibi güvenli alternatif yöntemler kullanılabilmelidir.

2.26. Ağ Güvenlik Duvarı Sistemi aktif dizin ile entegre edildiğinde ip/subnet/vlan/zone bazlı tanımlamalara ek olarak kullanıcı ve grup bazlı güvenlik politikaları yazılmasını desteklemelidir. Kullanıcı ve grup tanımlamaları politika ekranından arkadaki aktif dizin üzerinden otomatik filtrelenerek getirilen user, security group veya OU tanımları içerisinden çoklu-seçim ile tek adımda gerçekleştirilebilmelidir. Bu sayede farklı kullanıcı profillerine farklı güvenlik politikaları uygulanabilmelidir.

2.27. Ağ Güvenlik Duvarı Sistemi üzerinde güvenlik politikaları ip/subnet, interface (fiziksel/VLAN), zone, kullanıcı, grup (OU veya Security Group) haricinde cihaz tipi bazlı da yazılabilmelidir. Windows, Linux, Android, Iphone vb.. gibi hazır tanımlı cihaz kategoriler haricinde kişiselliştirilmiş cihaz tanımlamaları (el terminalleri, printer vb..) yapılabilmelidir.

2.28. Sistemin uygulama kontrol özelliği bulunmalıdır. Sistem; Mesajlaşma (MSN, ICQ, Yahoo, AOL gibi), P2P (Kazaa, Skype, bitTorrent, eDonkey, Gnutella vb) ve Web Uygulamaları gibi tanımlı en az 3.000 (üçbin) adet uygulamaya ait trafiği kullanılan porttan bağımsız olarak tanıyabilmeli, kontrol edebilmeli ve engelleyebilmelidir. Uygulama kontrolü kapsamında tanınan uygulamalar internet üzerinden güncelleme servisi ile güncellenmelidir.

2.29. Ağ Güvenlik Duvarı Sistemi Web 2.0 uygulamaları içerisindeki alt uygulamaları (facebook.chat, facebook.games vb.. gibi) ayırt edebilmeli ve sosyal medya uygulamalarına read-only erişimi (facebook açılsın ama oyun oynanamasın, chat fonksiyonu kullanılamasin vb.. gibi) mümkün kılabilmelidir.

2.30. Ağ Güvenlik Duvarı Sistemi uygulama veya kategori bazlı blok, reset, allow, log, karantina aksiyonlarını alabilmelidir.

2.31. Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında uygulama kontrol politikası set edilebilmelidir.

2.32.

2.33. Sistem VPN Gateway olarak IPSec VPN desteklemelidir. DES, 3DES, AES Kriptolama ile MD5 ve SHA-1 desteklemelidir. IKE ve PKI desteği olmalıdır.

2.34. IPS sistemi Trafik ve Protokol anomalilerini tespit edip durdurabildiği gibi, imza tabanlı saldırıları da tanıyıp durdurabilmelidir. IPS imzaları otomatik olarak internet üzerinden güncelleme servisi ile güncellenebilmelidir. Güncelleme işlemi manuel olarak ta yapılabilmelidir.

2.35. IPS sistemi en az 7000 (yedibin) imzaya sahip olmalıdır.

2.36. Teklif edilen sistem istenilen atak türleri gerçekleştiğinde bu atakları sadece engellemekle kalmayıp, atak kaynağını belli bir süre engelleyebilecek şekilde yapılandırılabilmelidir. Bu sayede atak yapan IP adresinin olası diğer saldırıları başlamadan engellenmiş olmalıdır.

2.37. Teklif edilen sistem istenilen atak türleri gerçekleştiğinde bu atakları sadece engellemekle kalmayıp, atak kaynağını ve aynı zamanda atak yapılan sistemlere olan erişimi belli bir süre engelleyebilecek şekilde yapılandırılabilmelidir. Bu sayede atak yapılan sistem olası ataklara karşı koruma altına alınabilmelidir

2.38. Sistem yöneticilerinin kuruma/ihtiyaca özel zaafiyet imzaları yaratıp bloklama yapabilmelerine imkân sağlamalıdır.

2.39. Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında IPS politikası set edilebilmelidir.

2.40. Teklif edilen Ağ güvenlik sistemi Botnet aktivitesini tespit edip engelleyebilmelidir.

2.41. Ağ Güvenliği Sistemi üzerinde, Mobil Kullanıcıların Kurum kaynaklarına güvenli olarak erişimini sağlayabilmek için, SSL VPN Gateway özelliği bulunmalıdır. SSL VPN istemcisi en az Windows, Mac OS, Linux işletim sistemlerini ve IOS, Android tabanlı mobil cihazları desteklemelidir.

2.42. SSL VPN Gateway içerisinden TCP ve UDP tabanlı trafikler tünellenebilmelidir.

2.43. SSL VPN özelliği en az 500 kullanıcı lisansı ile teklif edilecektir.

2.44. SSL VPN üzerinden erişen kullanıcılar, Sistem üzerinde tanımlı kullanıcı veritabanı, RADIUS, LDAP üzerinden kimlikleri doğrulanabilmeli, yetkilendirilebilmeli ve bu yetkilendirme ile erişilebilecek kurum içi ve dışı kaynaklar tanımlanabilmelidir.

2.45. SSL VPN ile erişim sağlayan kullanıcı veya sistemleri için; SPI (stateful packet inspection), Saldırı Tespit ve Engelleme Sistemi (IPS), Uygulama Tanıma ve Kontrolü (Application Control) Sistemi, Virüs/Zararlı İçerik Kontrolü ve URL Kategori Filtreleme, Bant Genişliği yönetimi (QoS) özellikleri uygulanabilir olmalıdır.

2.46. Ağ Güvenlik Duvarı Sistemi üzerinde zararlı yazılım (Malware) tespit ve engelleme özelliği bulunmalıdır. Sistem; HTTP, SMTP, FTP ve POP3 trafiğini tarayarak zararlı yazılımları engelleyebilmelidir. Sistem, anılan protokoller içinde tarama yaparak; Worm, Trojan, Keylogger, Spy, Dialer türünden tehditleri tanıyıp durdurabilmelidir. Virüs Kontrolü, Ağ Güvenlik Duvarı Sistemi üzerinde bulunan bütün network segment'leri arasında yapılabilmelidir. AntiVirus sistemi Internet üzerinden virüs imzalarını otomatik olarak güncelleyebilmelidir

2.47. Kaynak (IP ve/veya kullanıcı), hedef, servis bazında yazılan her güvenlik duvarı kuralında AV kontrol politikası set edilebilmelidir.

2.48. Ağ Güvenliği Sistemi üzerinde URL Filtreleme özelliği bulunmalıdır. Bu sayede Kategori bazlı URL Filtreleme yapabilmelidir. Farklı kullanıcı ve kullanıcı gruplarına farklı kategorilerde URL filtreleme uygulanabilmelidir.

2.49. Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında farklı domain adı filtreleme politikaları set edilebilmelidir.

2.50. Sistem üzerinde en az 70 adet URL kategorisi bulunmalıdır, en az 250milyon URL sınıflandırılmış olmalıdır.

2.51. Sistemin URL Filtreleme fonksiyonu için kullanıcı sınırı olmamalı ve sınırsız kullanıcı lisansı ile teklif edilmelidir.

2.52. URL filtreleme kategorileri dışında, wildcard, regex veya tam URL olarak istenilen adreslerin farklı profiller altında tanımları yapılabilmelidir (Örneğin *.gov.tr* gibi). Tanımı yapılan bu adreslere erişim engellenebilmeli veya izin verilebilmelidir.

2.53. Https üzerinden erişilmeye çalışılan domain adreslerinin (örneğin www.abc.com) engellemesi sertifika kullanımı olmadan gerçekleştirilebilmelidir.
2.54. SSL trafiğini kendi üzerinde yaratılan bir sertifikayı yada farklı bir CA den alınmış yeterli özelliklere sahip bir sertifika ile inceleyebilmelidir. Bu sayede sadece domain bazında değil, URL bazında (Örneğin: www.abc.com/deneme/test.php) engelleme yapabilmelidir. URL kategorileri bazında SSL incelemeye girmeyecek domainler belirlenebilmelidir.
2.55. URL/Application kontrol/Anivirus filtreleme uyarı ekranları özelleştirilebilecektir.
2.56. Teklif edilen tüm sistemlerin IPv6 desteği bulunmalıdır ve IPv4 ile IPv6 protokollerinin aynı anda kullanımına izin veren dual-stack özelliği desteklenmelidir. IPv6 kapsamında en az; IPv6 adresleme, IPv6 statik yönlendirme, IPv6 DNS, IPv6 güvenlik kuralları, IPv6 kayıt ve raporlama ve Ping6 desteklenmelidir.
2.57. Sistem IPv6 için DDoS profiline sahip olmalıdır.
2.58. Sistem yapılandırması en az aşağıdaki yöntemler ile yapılabilmelidir:
2.59. Seri bağlantı ile konsol port üzerinden,
2.60. Http ve Https bağlantı ile web ara yüz üzerinden veya üreticinin kendisine ait Linux veya Windows tabanlı yönetim uygulaması üzerinden
2.61. SSH bağlantı ile komut satırı (commandline) üzerinden
2.62. Ağ Güvenlik Duvarı Sistemin SNMP desteği olmalı ve SNMPv3 desteklemelidir
2.63. Ağ Güvenlik Duvarı Sistemi işletim sistemi ve yazılım güncellemelerini Web ara yüzü, TFTP veya FTP üzerinden yapılabilmelidir.
2.64. Yedekli olarak çalışan sistemlerin güncellemeleri en az web gui üzerinden yapılabilmelidir. Sistemler otomatik olarak, trafiği kesintiye uğratmayacak şekilde sırayla güncellenebilmelidir.
2.65. Güvenlik Duvarı Sisteminin coğrafi veri tabanı bulunmalıdır. Ülke bazında kural yazılarak belirtilen ülke veya ülkelerden gelen trafiği kesebilmelidir.
2.66. Teklif edilen güvenlik sistemi, aynı zamanda yük dengeliyici özelliklerine sahip olacaktır.
2.67. Sistem, içeri doğru NAT Load-Balance özelliği ile internetten gelen istekleri birden fazla sunucuya yönlendirebilmelidir. Örneğin, iç ağda bulunan ve aynı servisi veren iki web server veya terminal server arasında trafik paylaşımı bu özellik sayesinde yapılabilmelidir. Eğer web server veya terminal server'lardan birisi devre dışı kalırsa diğer web server veya terminal server herhangi bir müdahaleye gerek kalmadan hizmetine devam edebilmelidir.
2.68. Layer 7 için HTTP, HTTPS, SSL, Layer 4 için TCP ve UDP, Layer 3 için IP protokolü bazında tüm oturumlar için yük dengelemesi yapabilmelidir.
2.69. Yük dengelemesi uygulanan sunucular için IPS, AV politikaları kullanılabilmelidir.
2.70. HTTP, HTTPS bağlantıları için fiziksel sunuculara kaynak IP adresinin gitmesi sağlanabilmelidir.
2.71. SSL bağlantıları için SSL Offloading özelliği olmalıdır.
2.72. Trafik kurum gerçek sunucularına aşağıdaki yöntemlerle dağıtılabilmelidir:
2.73. Kaynak Ip hash bilgisi
2.74. Round robin
2.75. Sunucuların farklı güçlerde olabilme ihtimaline karşı gerçek sunucu tanımlarında ağırlık tanımı yapılarak
2.76. Aktif durumda olan gerçek sunuculardan ilkine trafiğin gönderilip, devre dışı kalması durumunda sonraki aktif sunucuya yükün gönderimesi
2.77. Ping paketlerine verilen cevaplar esas alınması
2.78. Sunucular üzerine yönlendirilen session sayı bilgisine bağlı olarak
2.79. Yük paylaşımı sırasında sunucu bulunurluğunu tcp, http (örneğin http://10.31.101.30/test_page.htm adresinin kontrolü ile) ve ping ile kontrol edebilmelidir.
2.80. Explicit proxy özelliği desteklenmelidir.
2.81. Sistem TCP eşik değeri temelli DoS/DDoS koruması saglayabilmelidir.
2.82. 10 adet sanal güvenlik duvarı desteği standart lisans ile verilebilmelidir.
2.83. Sistem WAN tarafında optimizasyon ve yük dağılımı desteği olmalıdır.

2.84. Sistem wan link load balance özelliğine sahip olmalıdır ve internet çıkışı oransal olarak ilgili dış hatlara yönlendirilebilmelidir.
2.85. Common Internet File System (CIFS), FTP, HTTP, MAPI ve TCP oturumları için protokol optimizasyonu yapabilmelidir.
2.86. Web cache özelliği olmalıdır.
2.87. Sistem WAF (Web Application Firewall) profillerini desteklemelidir. Bu oluşturulan profiller kural temelli olarak tanımlanabilmelidir.
2.88. Web cache communication Protocol (WCCP/ICAP) desteği olmalıdır.
2.89. Sistem WAF (Web Application Firewall) profillerini desteklemelidir. Bu oluşturulan profiller kural temelli olarak tanımlanabilmelidir.
2.90. Sistem VOIP güvenlik profillerine sahip olmalıdır ve kural temelli olarak uygulanabilmelidir.

b. Güvenlik Duvarı Performans Değerleri

2.91. Teklif edilen Ağ Güvenlik Duvarı, yedekli aktif-aktif/aktif-pasif olarak çalışabilme özelliğine sahip olmalıdır.
2.92. Teklif edilen güvenlik sistemi, teklif edilen konfigürasyonda, 1518/512/64 Byte IP paket büyüklüklerinin hepsi için en az 10 Gbit/sec performansı değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili belgelerinde belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
2.93. Sistem aynı anda en az 1 milyon oturumu desteklemeli ve saniyede en az 50 bin yeni oturum açabilme performansına sahip olmalıdır. Bu değerler teklif edilen ürün dokümanlarında belirtilmiş olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
2.94. Güvenlik Duvarı Sistemi en az 10 Gbit IPSec VPN throughput değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
2.95. Güvenlik Duvarı Sistemi en az 1Gbit SSL inspection throughput değerine sahip olmalıdır. Bu performans degieri IPS açık iken HTTP trafiğinin TLS v1.2 with AES256-SHA şifrelemesi ile elde edilmelidir. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
2.96. Sistem Site-to-Site için en az 1000 adet, Client to site için 2000 adet IPSec VPN tünel desteklemelidir. Cihaz, anılan VPN protokollerini destekleyen standartlarla uyumlu VPN Gateway cihazları ile uyumlu çalışabilmelidir
2.97. Sistem 2Gbit/sec Enterprise MIX IPS throughput performans değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
2.98. Sistem 1Gbit/sec Thread Prevention (Malware kontrol, Application kontrol, IPS) throughput performans değerine Enterprise trafic MIX veya gerçek trafik değeri olarak sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
2.99. Sistemin; Firewall, VPN, IPS fonksiyonlarının hiç biri için kullanıcı sınırı olmamalıdır ve sınırsız kullanıcı lisansı ile teklif edilmelidir. Ağ Güvenlik Sisteminin 3 (Üç) yıl süre ile Yazılım/işletim sistemi güncellemelerini ve en az 3 (Üç) yıl süre için IPS, Uygulama Tanıma ve Kontrolü, AntiVirus, URL Kategori Filtreleme servis ve güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.

3. Network Otomasyon Monitör Yazılımı

3.1. Teklif edilecek yazılımı Yerli ve Milli Belgesine sahip olacaktır.
3.2. Teklif edilecek yazılım en az 1000 Cihaza kadar lisanslama kapasitesi olacaktır.
3.3. Ağ Ekipmanlarının, VM'lerin ve ayrıca DB, ağ bağdaştırıcıları vb. ilgili yazılım öğelerinin kaynak tüketimi ayrıntılarıyla birlikte listelenecektir.
3.4. Temel Teknik özellikler içerisinde tanımlanmış olan kısımlar tamamı ile kurum istekleri doğrultusunda, üreticinin zaruri görmesi halinde değiştirilebilir olmalıdır. Bu değişiklikler:

- Bir özelliğin farklı bir sayfaya alınması
- Yazılım renklerinin değiştirilmesi
- Bir sayfa içerisindeki bilgilerin arttırılması ve azaltılması
- Bir sayfa içerisindeki bilgilerin yerlerinin değiştirilmesi
- Talep halinde Türkçe dil desteğinin geliştirilebilmesi
- Talep edildiğinde kurum logosunun eklenmesi
- Entegrasyonu gerçekleştirilecek olan üretici ürün ailesi kontrol yazılımından gelen cihazlara yönelik talep halinde ekstra geliştirmelerin yapılabilmesi
- Kurum içerisinde ve yine kuruma özel bir yazılım var ise Entegrasyon alanına bu yazılımın logosu ile tam entegrasyonunun yapılabilmesi

3.5. Ürüne ait Türkçe kullanım kılavuzu olmalıdır.
3.6. Multitenancy (Çoklu Kullanıcılık) desteklenecektir.
3.7. Yazılıma aynı anda birden fazla kullanıcı bağlanabilecektir. Bağlanacak kullanıcı sayısı belirtilmelidir.
3.8. Teklif edilecek yazılım Cisco NSO yazılımı ile entegre olabilecektir.
3.9. Temel Özellikler:
3.10. Sisteme ait genel durum bilgilerinin bulunduğu bir ana sayfaya sahip olacaktır. Bu sayfada gösterilecek olan özellikler aşağıdakilerden az olamaz ve kurumdan gelecek olan istekleri karşılayacak şekilde gereken geliştirmeler ve bu sayfaya yansıtmalar yapılabilmelidir:

- Sisteme anlık kayıtlı olan cihaz adeti
- Sisteme kayıtlı olan cihazların anlık durumlarını ayrımlı olarak gösteren bir alan
- Sisteme kayıtlı olan cihaz türlerine ait bir genel görüntü
- Sistem içerisinde gerçekleştirilmekte olan işlemlerin gösterildiği bir alan (örneğin topolojinin güncellenmesine ilişkin bir durum çubuğu)
- Sistem içerisinde tanımlanmış olan Kural Bazlı Otomasyon a yönelik bilgilendirme Alanı
- İçeriğini sağlayabilen üreticiler için Güvenlik Önerileri
- Sisteme gelen Alarm ile ilgili bilgilendirme Alanı

3.11. Sisteme eklenmiş olan cihazlar arasındaki bağlantıları IEEE standartlarına göre otomatik olarak çizebilen bir Topology ekranı olmalıdır. Bu alanda gösterilecek olan bilgiler aşağıdakilerden az olamaz ve kurumdan gelecek olan taleplere göre geliştirilebilmelidir:

- Cihazlar tiplerine göre uygun olan resimler ile sembolize edilmelidir
- Cihaz üzerine gelindiğinde cihaz ile alakalı olarak bilgiler gösterilmelidir
- Cihazların birbirleri ile olan bağlantılarının üstüne gelindiğinde; bağlı olan cihazlar ve hangi portlar ile bağlandığının bilgisi gösterilmelidir
- Cihaz bağlantıları beyaz bir sayfada ve istenildiği takdirde Dünya Haritası üzerinde gösterilebilmelidir.
- Topology ve burada yer alan cihazlara ilişkin detaylı bilgi veren başka bir alanı sayfa olarak barındırmalıdır.
- Topology üzerinde yer alan cihazlara tıklandığında başka bir alanda cihaza ve bağlantılarına ait detaylı bilgiler görüntülenebilmelidir.
- Topology belirli aralıklar ile güncellenebilmelidir. Bu güncellemenin hangi aralıklar ile yapıldığı bilgisi kuru mile paylaşılmalıdır.

- Sisteme manuel olarak eklenen cihazlara ait Topology bilgisi gösterilebildiği gibi herhangi bir yönetim yazılımı entegrasyonun ile gelen başka bir topology bilgisinin de gösterilebildiği seçimli bir alan olmalıdır.
- Sistem gerektiğinde aradaki bağlantıları gerektiğinde de bağlantılar dışında cihazların sadece lokasyonlarını gösterecek şekilde gereken ayarların yapılmasına izin verebilir olacaktır.

3.12. Envanter Alanı içerisinde bulunması gereken alanlar aşağıda açıkça belirtilenlerden az olamazlar:

- Tüm cihazların gösterildiği bir alan
- Cihazlara bağlanmak için kullanılacak olan protokollerin tanımlamalarının yapıldığı bir alan
- Sisteme tanımlanan cihazlara kurum isteklerine göre eklenecek olan özel etiketlerin tanımlamalarının yapıldığı bir alan
- Sistem içerisinde tanımlı olan cihazlar arasında seçimlilik Alanı (Manuel ve başka bir yönetim yazılımı içerisinden sisteme entegre edilmiş cihazlar arasında geçişi anlayan bir menü)
- Yeni cihaz eklenme Alanı
- Seçilen cihazın silinebilmesi
- Otomatik olarak envanter keşfi alanı
- Çoklu cihaz tanımlamasının yapılabilmesine olanak sağlayan CSV formatı ile envanter yükleme Alanı

3.13. Sisteme entegre edilmiş olan cihazlardan çekilecek ve ekranda gösterilecek olan bilgiler aşağıdakilerden az olamazlar. Ancak kurumdan gelecek olan talebe göre gereken eksiltme ve arttırma geliştirilebilmeli, ilgili ekrana yansıtılabilmelidir.

- Cihaza ulaşılabilirlik durumu
- IP adresi (Filtreleme özelliği olmalıdır)
- Cihaz adi (Filtreleme özelliği olmalıdır)
- Yazılım versiyonu
- Seri numarası

3.14. Ürün tipi (Kurum bu alanda ürünün tipine göre seçimlilik yaparak sadece seçtiği ürünlerin bilgilerinin görüntüleyebilmelidir)

3.15. Cihazın anlık durumu (Sistemin hangi aralıklar ile cihaz durumunu kontrol ettiği ve ekrana yansıttığı ayrıca belirtilecektir ve kurum cihazın durum bilgisine göre filtreleme yapabilecektir.)

3.16. Seçilen cihaz ile ilgili değişiklik, silme ve detaylı bilgiye ulaşılacak bir alan

3.17. Kurumdan istek geldiği takdirde cihaza tanımlanan özel bir etiket var ise onun gösterildiği bir satir (Birden fazla etiket tanımlandığı durumlarda kurum etiketler arasında gerek tek gerekse çoklu seçimlilik yaparak ekranda ilgili etikete sahip cihazların bilgilerini görebilmelidir)

3.18. Sistem içerisine dahil edilmiş olan tüm cihazlara ait SNMP bilgilerinin monitör edilebildiği alandır.

3.19. Bu alan içerisinde monitörlere işleminin gerçekleştirileceği cihazların tam listesi olmalıdır.

3.20. Liste içerisinde yer alan cihaz seçildiğinde o cihaza ilişkin olarak hangi SNMP bilgisinin monitorleneceği bilgisi görüntülenebilmelidir.

- Monitorleme ekranı içerisinde yer alacak bilgiler temelde:
- CPU
- Memory
- Harddisk
- Power
- Interface Bilgileri

3.21. Monitörlere bilgileri herhangi bir yazılım kullanılarak ekrana yansıtıldığı takdirde tam ekran olarak gösterilecektir.
3.22. Sistem içerisinde cihaz tanımlanır tanımlanmaz çekilecek olan SNMP bilgilerine yönelik isimlerin gösterildiği bir alan bulunacaktır.
3.23. Musteri bir cihaz bilgilerine ulaşmak için ilgili alana gittiğinde o alan içerisinden çıkmadan, cihaz ismi ve o cihazın arayüzünü seçerek Ağ Ekipmanları içerisinde seçimlilik yaparak ilgili bilgileri görüntüleyebilecektir.
3.24. Teklif edilecek olan yazılım Kural Tabanlı Otomasyon destekleyecektir. Bu özellik için ayrı bir sayfası ve ayrı bir raporlaması olacaktır. Desteklenecek olan genel özellikler aşağıdaki maddelerden az olmayacaktır:
3.25. Yapı içerisindeki algoritma farklı kaynaklardan olay (evet) toplayabilecektir.
3.26. Arayüz üzerinden bir olay karsısında alınacak olan aksiyon tanımlaması yapılabilecektir.
3.27. Daha önceden tanımlanmış olan kuralların çıktılarına göre diğer kuralları çalıştırabilecektir.
3.28. Tanımlanmış olan kurallar otomatik olarak çalışacaktır.
3.29. Netçin protokolü ile cihaz üzerinde değişiklik yapabilecektir.
3.30. Web Servisleri veya API larp için http istek yapabilme özelliği desteklenecektir.
3.31. Restken protokol desteği bulunacaktır
3.32. Almış olduğu alarmları otomatik çeliştirdiği kuralları E-Posta ile bilgilendirme özelliği bulunacaktır.
3.33. SSHv2 protokolü aracılığı ile tanımlanan kural içerisindeki değişiklikleri cihazlara iletebilecektir.
3.34. Otomatik olarak çeliştirilmiş olan kurallara yönelik alarm tanımlamaları yapılabilecektir.
3.35. Alarm lain karşılığında çalıştırılacak olan kurallar için zaman tanımlaması yapılarak, istenilen zamanda istenilen kural in çeliştirilmesi sağlanabilecektir.
3.36. Kullanılan ve üzerinde hâlihazırda tanımlanmış olan kuralları System çağırıp gereken aksiyonu otomatik olarak alabilecektir.
3.37. Yazılım içerisine gerek manuel gerekse entegrasyonlar ile gelen tüm cihazların bir arada bulunduğu ve bu cihazlar üzerinde gerekli işlemlerin yapıldığı ve kullanıcı ya da yöneticinin tüm cihazlar hakkında detaylı bilgiye ulaştığı bir alan bulunmalıdır.
3.38. Teklif edilecek yazılım Envanter yönetiminin diğer ekranları ile entegre olarak kullanıcı ya da yöneticiyi bilgilendirdiği bir özet alana sahip olacaktır. Alan içerisinde kulun maşı gerekenler aşağıdakilerden az olamazlar:

- Genel bir bilgilendirme (özet) Alanı
- Tüm envanterin görüntülenebildiği ayrı bir sayfa
- Destekleyen üreticiler için güncel Bug bilgilendirme sayfası
- Destekleyen üreticiler için güncel güvenlik açıkları bilgilendirme sayfası
- Konfigürasyon yedeklerinin alınmasına olanak veren bir sayfa
- Raporlama sayfası

3.39. Sistem ile ilgili tanımlamaların yapıldığı ve genel bilgilendirmelerin de gerek duyulduğunda eklenebileceği bir Yönetici arayüzü olmalıdır. Bu yönetici arayüzü aşağıdaki kapsamı en az karşılayacak şekilde olmalıdır:

- Entegrasyonlar
- Kullanıcı Tanımlamaları ekranı
- AAA entegrasyonları Alanı
- Genel Sistem İşlemleri bilgilendirme ekranı
- Sistem hakkındaki genel bilgilendirme ekranı
- Sistem içerikleri kapasite bilgilendirme ekranı
- Sistemde yapılan işlemlerin kayıt altına alındığı bir alan

3.40. Sistem içerisinde gerçeklesen olay (EVENT) ve gerek kendisinin yarattığı gerekse kendisine entegre olan sistemlerden aldığı Alarmları gösterdiği bir alana sahip olmalıdır. Bu alan aşağıdaki ekranlardan daha azını barındıramaz:

- Olay ekranı (EVENT)
- Alarm Ekranı
- Sistem Bilgi Zenginleştirme ekranı
- Yukarıda sıralanmış alanlar ve içerikleri kurumdan gelecek taleplere istinaden değiştirilebilir olacaktır.

Teknik Özellikler

3.41. Teklif edilecek yazılım aşağıda tanımlandığı şekilde cihaz eklemesi yapabilmelidir:

- Cihaz ulaşım bilgilerinin tanımlanacağı alan için sistem üzerinde bir isim tanımlanabilmelidir ve cihaz ekleme ekranında bu isme göre secim gerçekleştirilebilmelidir.
- Cihaz eklenmesi için gerekli olan tanımlamaların (SSH, SNMPv2 vb..) yapılabilmesi için ayrı bir arayüz olmalıdır.
- Yapılmış olan tanımlamaların silinmesi ve değiştirilmesi için yazılım içerisinde tanımlanmış olan tanımlamaların yanında ilgili alan bulunmalıdır.
- Aşağıdaki gereksinimler tek bir ekran üzerinden yapılabilmelidir.
    a. Cihaz sisteme yönetim IP adresinden veya kurum içerisinden ulaşılan ip adresinden tanıtılabilecektir.
    b. Cihaza yazılımın ulaşabilmesi için gereken sah, snmpv2 gibi protokollerin daha önceden yapılan tanımlamaları tek bir isim ile bu alan içerisinde görülüp seçilebilmelidir.
    c. Cihaza bağlanmak için kullanılacak olan protokoller sah, snmp vb. aşağıya doğru kayan bir menüde seçilebilmeli ve bu secimden sonra sistemin bu bağlantı için kullanacağı port numarası otomatik olarak görülebilmelidir.
    d. Tanımlanan cihazın otomatik olarak Topology ekranında dünya haritası üzerinde görüntülenebilmesi için aşağıdaki tanımlamalar yine ayni ekran üzerinde yapılabilmelidir. Bunlar:
        a. Bina
        b. Cadde
        c. Şehir
        d. Ülke
        e. Posta Kodu
        f. Coğrafi Koordinatlar (Latitude, Longitude)
    e. Ayni sayfa içerisinde sisteme eklenmiş olan cihazlara ait olan ve otomatik olarak çekilen bilgilerin gösterildiği bir alan bulunacaktır.
    f. Yukarıda tanımlaması yapılmış olan özellikler silinebilmeli ve değiştirilebilmelidir. Yapılacak olan bu değişiklerden sistem kesinlikle etkilenmeyecektir.

3.42. Teklif edilecek yazılım aşağıda detayları verilmiş olan entegrasyon özelliklerine sahip olmalıdır:
Teklif edilecek olan yazılım kurum içerisinde kullanılıp kullanılmamasına bakılmaksızın aşağıdaki sistemler ile sorunsuz bir şekilde entegre olmalıdır:

- Sybelle
- Vmware Vcenter
- Aruba Mobility Controller
- Cisco (ACI, UCS Manager, DNA Center, SDWAN, Meraki ve CNC)
- SMTP
- Cisco Webex
- Microsoft Teams
- Slack
- Wrike
- Jira
- Jira Service Management
- Zabbix ve Grafana
- Servis ve Destek bilgilendirme entegrasyonları (Desteği olan üreticiler için)

3.43. Teklif edilecek yazılım envanter içerisinde yer alan cihazlardan destek verdikleri takdirde konfigürasyon yedeklemesine sahip olacaktır. Bu yedekleme;
3.44. Günlük, haftalık ve aylık olarak ayarlanabilecektir.
3.45. Envanter içerisindeki cihazlardan gruplama mantığı ile yedek alabilecektir.
3.46. Periyodik olarak yedekleme tanımlanabilecektir.
3.47. Periyodik olarak saat bazlı yedek alabilecektir.
3.48. Anlık olarak herhangi bir cihazdan yedek alabilecektir.
3.49. Anlık alınan yedek ile daha önceden alinmiş yedek arasındaki farkları gösterebilecektir.
3.50. Alınacak yedek adeti belirlenebilecektir.
3.51. Yedekleme işlemi için tanımlanan havuz gerektiğinde işlevsiz hale manuel olarak getirilebilecektir.
3.52. Teklif edilecek olan yazılım sisteme dahil edilmiş olan cihazlara yönelik almış olduğu konfigürasyon yedeklerini karşılaştırma yapma fonksiyonu dışında gösterebilecektir.
3.53. Teklif edilecek olan yazılım kendisine tanımlanmış olan cihazlara SSHv2 kullanarak bağlanarak kurulum yapılmasına izin verecektir. Bu bağlantı esnasında sistem herhangi bir kullanıcı adi veya şifre sorgulaması yapmayacaktır. İstekli kaç adet cihaza aynı anda bağlanılabildiğini ayrıntılı olarak verecektir.
3.54. 5.madde içerisinde tanımlanmış olan isterler talep edildiği takdirde kurumun ortamındaki güvenliği sağlayan başka bir merkezi yazılıma entegre edilerek de gerçeklenecektir
3.55. Teklif edilecek System içerisinde farklı kullanıcı grupları tanımlaması yapılabilecektir. Tanımlanan bu kullanıcı gruplarına yazılım içerisinde yer alan özellikler için kısıtlama tanımlanabilecektir.
3.56. Teklif edilecek yazılım içerisinde tanımlanan kullanıcı veya kullanıcı grupları içerisinde ayrı ayrı yetkilendirme ayrımı yapılabilecektir.
3.57. Yazılım üzerinde tanımlanmış olan uç nokta cihazlara Hız Testi yapılabilecektir. Bu işlem teklif edilecek olan yazılım üzerinde gerçekleştirilecektir.
3.58. Raporlama desteği olacaktır. Firma yazılımının bu alan içerisinde sağladığı Teknik faydaları ayrıntılı olarak açıklayacaktır.
3.59. Raporlama arayüzü istenildiği takdirde değiştirilebilir ve kapsamı genişletilebilir olmalıdır. Buradaki değişimlerin güncelleme ile sisteme eklenmesi için gerekecek sure istekli firma tarafından açıkça belirtilecektir.

3.60. Teklif edilecek yazılım SNMP Trap alabilecektir.
3.61. Teklif edilecek yazılım iki turlu kullanıcı kabulünü destekleyecektir (Two-Factory Authentication). İstekli desteklenen mekanizmasını detaylı olarak açıklayacaktır.
3.62. Teklif edilecek olan yazılım, 1 yıllık 8x5 NBD (Next Business Day- en geç ertesi iş günü müdahale) destek paketiyle birlikte teklif edilecektir.
3.63. Üretici desteği Türkçe Dilde verilecektir.
3.64. Destek personelleri üreticinin yetkili kıldığı, sertifikalı iş ortakları tarafından ve/veya doğrudan üreticinin ekibi tarafından sağlanacaktır.
3.65. Teklif edilecek olan ürün içerisinde kurumdan gelecek olan geliştirme talepleri, Üretici kabul ederse ekstra ücretlendirmeyle yapabilecektir.